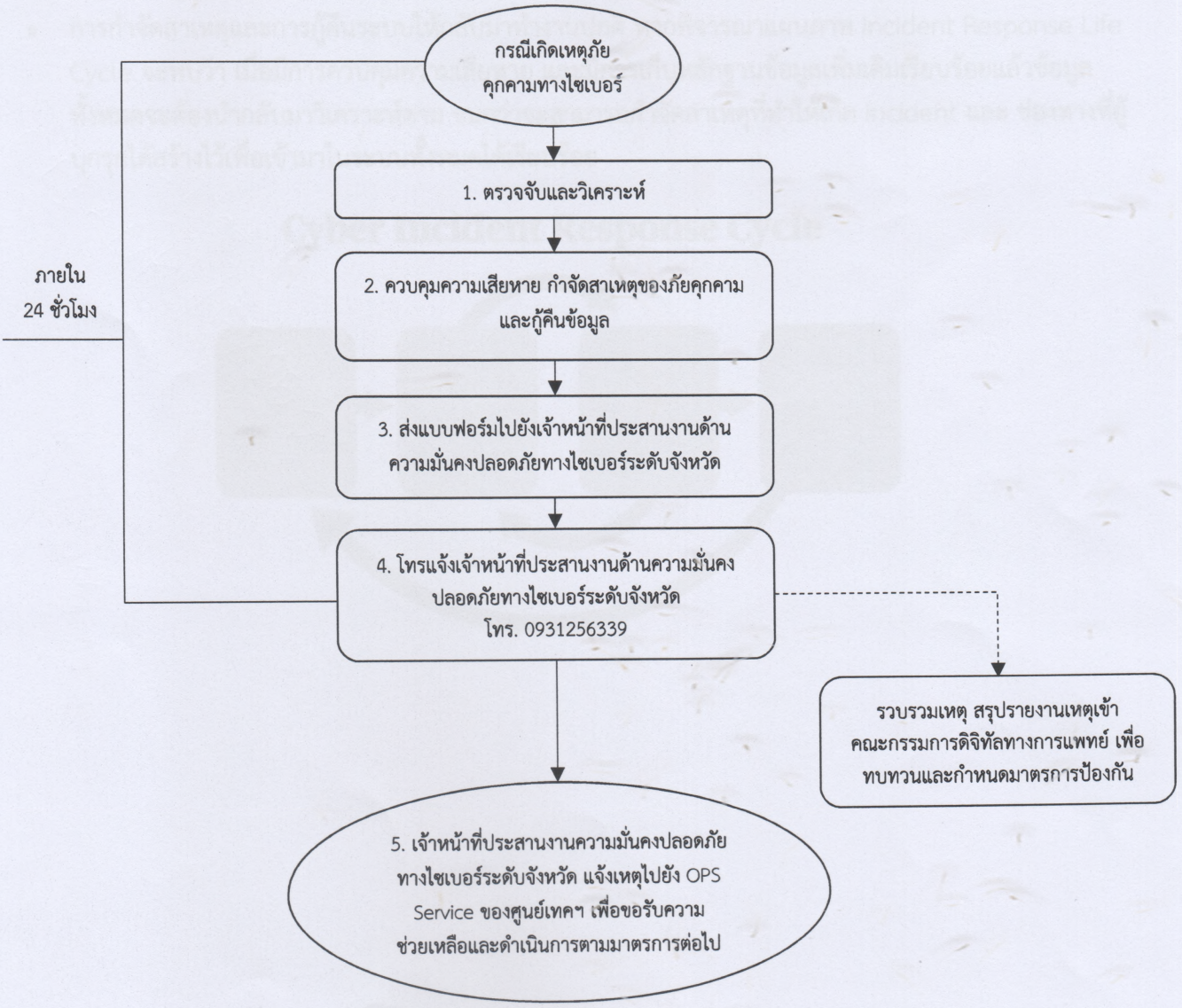
โรงพยาบาลวัฒนานคร จังหวัดสระแก้ว	**หน้า:** 1/1
นโยบายและระเบียบปฏิบัติเลขที่: PR-IM-120	**ฉบับที่:** 1/66 **แก้ไขครั้งที่:** -
เรื่อง: การแจ้งเหตุด้านความมั่นคงปลอดภัยทางไซเบอร์	**วันที่:** 17 มกราคม 2566
แผนก: กลุ่มงานประกันสุขภาพยุทธศาสตร์และสารสนเทศทางการแพทย์	**แผนกที่เกี่ยวข้อง:** สารสนเทศ
ผู้จัดทำ: คณะกรรมการ IM	**ผู้อนุมัติ:** ..... ผู้อำนวยการโรงพยาบาลวัฒนานคร
ผู้ทบทวน: ประธานทีม IM	

นโยบาย: เพื่อให้มีแนวปฏิบัติการแจ้งเหตุด้านสารสนเทศความมั่นคงปลอดภัยทางไซเบอร์

วัตถุประสงค์: เพื่อให้เจ้าหน้าที่ประสานงานความมั่นคงปลอดภัยทางไซเบอร์ได้ถูกต้องตามขั้นตอน

แนวปฏิบัติ: ประสานการดำเนินงาน แจ้งเหตุด้านความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานแก่ผู้ประสานงานการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับจังหวัดภายใน 24 ชั่วโมง

Flowchart การแจ้งเหตุด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)



การควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคาม และการกู้คืน (Containment, Eradication & Recovery)

- พิจารณาวิธีการในการควบคุมความเสียหาย การควบคุมความเสียหายมีความจำเป็นอย่างยิ่งที่จะป้องกันไม่ให้ความเสียหายกระจายออกไปเป็นวงกว้าง สร้างผลกระทบต่อทรัพยากรในการดำเนินธุรกิจอื่น ๆ และยังเป็นการเปิดพื้นที่ เพิ่มระยะเวลาให้ทีมที่รับมือ Incident มีเวลาในการคิดหาสาเหตุ และวิธีการแก้ปัญหาที่ถาวรได้ ข้อสำคัญของการควบคุมความเสียหาย คือการตัดสินใจเลือกใช้วิธีการที่เหมาะสม โดยวิธีการทั่วไปมีดังต่อไปนี้
    - ปิดระบบ (Shut Down)
    - ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network disconnection) ทั้งนี้ อาจมียกเว้นการเชื่อมต่อสำหรับ Endpoint Detection & Response Agent (กระบวนการตรวจสอบและตรวจจับกิจกรรมหรือเหตุการณ์ที่น่าสงสัยใด ๆ ที่เกิดขึ้นที่ ปลายทางแบบเรียลไทม์)
    - หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions)
    - Redirect Network Traffic และ/หรือความสนใจของผู้บุกรุกไปยัง Blackhole/ Sandbox/ Honeypot
- การจัดเก็บและดูแลรักษาหลักฐานทางดิจิทัล วัตถุประสงค์หลักของการจัดเก็บหลักฐาน คือ เพื่อให้การแก้ไข Incident ส่งผลกระทบต่อกระบวนการทำงานให้น้อยที่สุด (Minimizing impact to the business)
- การกำจัดสาเหตุและการกู้คืนระบบให้กลับมาทำงานปกติ หากพิจารณาแผนภาพ Incident Response Life Cycle จะพบว่า เมื่อมีการควบคุมความเสียหาย และมีการเก็บหลักฐานข้อมูลเพิ่มเติมเรียบร้อยแล้วข้อมูลทั้งหมดจะต้องนำกลับมาวิเคราะห์ตาม จนกว่าจะสามารถกำจัดสาเหตุที่ทำให้เกิด Incident และ ช่องทางที่ผู้บุกรุกได้สร้างไว้เพื่อเข้ามาในระบบทั้งหมดได้เรียบร้อย